資料2-10

サポート終了製品のパートナーシップにおける取扱いに関する調査

サポート終了製品のパートナーシップにおける取扱いに関する調査

- パートナーシップの運用において、サポート終了製品の取扱いが明確となっていない部分および取扱いをする上での課題があるため、取扱いが停滞する場合がある。

- このため、明確となっていない部分と課題となっている部分についての運用及び改善方法について検討する。

(1) JPCERT/CCへのヒアリング

↓

(2)課題の改善策、新たな運用ルールのとりまとめ

・パートナーシップにおいてサポート終了製品の取扱いが明確となっていない部分および取扱いをする上での課題等

［調査項目の例］
- パートナーシップにおけるサポート終了した製品の定義
- サポート終了した製品の優先情報提供の実施方法
- サポート終了した製品の公表判定委員会での判定要否
- サポート終了した製品の公表手続き

検討の背景

- 現行で取扱いを実施している案件のなかに下記の状況を全て満たすものがある。
  - 製品開発者のウェブサイトにおいて、EoL宣言が公表されている；
  - EoL宣言で規定されるサポート終了期限を既に経過している；
  - EoLとなっているが、現時点においても重要インフラ事業者等で利用されている可能性がある（優先情報提供の候補案件）；
  - 当該EoL製品を組み込んだ製品が、当のEoLの製品開発者とは異なる者によって開発されており、この異なる製品開発者の製品も重要インフラ事業者等で利用されている可能性がある。
- EoL であることを理由に、製品開発者との調整が難航する可能性があったため、現場担当者間で取扱方針の検討を進めていた。
- その検討のなかで、取扱い（とりわけ優先情報提供）について、明確ではない点があることが判明したため、それらの整理・方針検討を実施したい。

課題整理

■ サポート終了製品のパートナーシップにおける取扱いに関する課題は以下の通り。

課題		検討結果
1	パートナーシップにおける サポート終了した製品の定義	• **過去脆弱性研究会で検討済**のため、改めて定義する必要はないと考えている。 • ただし、**課題２以降の検討をするにあたって、サポート終了（EoL）の定義を明確化する必要がでてきた際には検討をする必要がある**と考えている。
2	サポート終了した製品の 優先情報提供の実施方法	• 現在のガイドラインにおいては、**ベンダの了承を得た場合にしか提供できない**。サポート終了しているためベンダからの**了承の取得が困難**であり、優先情報提供をすることができない。 • ガイドラインの改訂（手続きの改善次第）で提供可能となる可能性があるため、**実施方法を検討・決定したい**。 • （例）公表判定委員会にて、優先情報提供の可否についても判定し、実施できることとしたい（現状では、サポート終了か否かを問わず、公表判定委員会判定案件は、告示・ガイドラインに規定がないため優先情報提供できない。）
3	サポート終了した製品の 公表判定委員会での判定要否	• **サポート終了について特別扱いしない**こととなっている（2016年度脆研で、公表することは検討済みのため） • そのため、サポート終了であっても公表判定委員会にかけることは可能であると認識している。
4	サポート終了した製品の 公表手続き	• 上記の項目3と同様

サポート終了した製品の優先情報提供の実施方法

■ JPCERT/CCとのヒアリング概要

JPCERT/CCに本件課題についてヒアリングした結果は下記の通り

- EoLであっても、連絡がとれる製品開発者であれば、そこで優先情報提供の了承を得ることが可能である。**課題となるのはEoLであってかつ連絡不能になるもの**だけではないか（下記表の整理）。
- 連絡不能になる場合、連絡不能開発者一覧への掲載など、一定の手続きを要するため、**早期対応には限界**がある。
- 「EoLであること」については、製品開発者のウェブサイト上で確認可能であるのであれば、この**早期警戒パートナーシップの枠組みに乗せることなく注意喚起を行う**方が、本パートナーシップ内での対応を検討するよりも効果的なのではないか。
- EoL製品の届出がある場合、そのEoL製品を組み込んで自社製品を開発している製品開発者に対しては、製品開発者として登録がなされているのであれば、「製品開発者」として、EoL製品の情報を受け取ることが現状で可能である。
- また、公表に至る前の段階（受理時点等）であっても、優先情報提供のスキームを利用し、脆弱性の概要を伏せたうえで、**「この製品は、EoLです。利用を停止してください。」という旨だけを情報提供する**ことも一案である。

■ 連絡不能とEoLの関係

課題有無	連絡が可能	連絡が不可能 (連絡不能)
EoLである	－ 連絡が取れるのであれば個別に同意をとればよい	○ 固有の課題がある
EoLでない	－ （通常の製品案件） 連絡が取れるのであれば個別に同意をとればよい	△ 連絡不能として取扱いがなされる （優先情報提供はできない） 対応方策によっては、取扱い・運用等に変更が生じる可能性がある

サポート終了した製品の優先情報提供の実施方法

- JPCERT/CCへのヒアリングを踏まえ、課題と対応方策を以下のように整理した。
  - 課題・認識
    - 連絡不能になる場合に優先情報提供が実施できないことは改善すべきである。
    - JVN公表・優先情報提供によるのではなく、それら以外の手法で、EoLであることを周知し利用停止を促すことで公表前の脆弱性悪用のリスク低減を図ることを検討する。

	対応方策案		備考
1	優先情報提供の条件を緩和する • 優先情報提供の条件を緩和し、EoL製品については、製品開発者の同意を得ずとも優先情報提供できるようにする		
	1-1	優先情報提供の条件の改訂（告示改正要） 連絡不能案件であって下記の条件のいずれかを満たす場合に優先情報提供を可能とする • 調整機関および受付機関の協議 • 経済産業省の了承 • 公表判定委員会での審議での了承	公表判定委員会の審議案件は、EoLではない通常の案件であっても、（製品開発者の了承が条件であるため）優先情報提供ができない。
	1-2	優先情報提供の条件解釈の緩和（告示改正不要） • 「協議」であり「合意」ではないことから、明示的な同意までは不要であり、EoLの宣言が公表されていることをもって、「協議」として十分であるとの整理する	「協議」の解釈については、経済産業省・法律家（高橋委員）に確認する必要がある

（※）告示　第2　2　(3) 調整機関　セ
調整機関は、対策方法が作成された日から脆弱性情報公表日までの間であって、国民の日常生活に必要不可欠なサービスを提供するための基盤となる設備に脆弱性に起因する重大な影響が及ぶおそれがあると認められるときは、受付機関及び製品開発者と協議をした上で、政府機関や当該設備を用いる事業者等（脆弱性情報等を適切に管理できる者に限る。）に当該脆弱性情報等をあらかじめ通知することができる。

サポート終了した製品の優先情報提供の実施方法

	対応方策案		備考
2	「EoL製品情報（脆弱性の存在有無については触れず、「EoLであること」と「利用停止を促す案内」を記載）」を提供する		
	2-1	優先情報提供のスキームを利用し、「EoL製品情報」を重要インフラ事業者等に提供する	
		• 本パートナーシップを経由した注意喚起をすることで、事業者側が利用を見直す契機となることが期待できる	
	2-2	JVN公表前に「EoL製品情報」を一般に公表する	
		• 届出を契機とする注意喚起はしてもよいのが問題となる。 • 製品開発者のウェブサイト上でEoL宣言が公表されている場合、届出とは無関係にEoL情報を確認した場合は、（本パートナーシップとは無関係に）注意喚起できるが、届出を機にEoL情報を確認した場合には、注意喚起できないとするのは不当ではないか。	
	2-3	ベンダリストに登録されている製品開発者に「EoL製品情報」を展開する	テクノロジーキーワードでの登録内容とは無関係に実施（キーワード登録をしていれば、現行で対応が可能）
		• 利用者である重要インフラ事業者等だけでなく、EoL製品を利用して自社製品を作成している製品開発者にもEoL情報を伝達するようにすべきである。	

その他の事項

■ その他

JPCERT/CCへのヒアリングで、EoL製品の取扱いと直接にかかわらない制度上の課題について指摘がなされた。

- 連絡不能開発者一覧に掲載するまでに、最短で一か月かかる。その後、再掲載し、検証、委員会の資料作成をすることとなるため、さら三か月ほどかかるが、半年弱での開催が可能ともいえる。優先情報提供の対象になるような案件については、審議対象案件が1件のみであっても、公表判定委員会を開催する意義があるのではないか。連絡回数がすくないのであれば、連絡の作業証跡が少なくて済むため、資料作成の工数は、過去の審議案件に比して少なくなる。

- 公表判定委員会の開催については、現在の対面形式ではなく、ビデオ会議やメール審議など、迅速に対応できる手法を検討すべきではないか。